

CLAIMS

- 1 1. A method of authenticating a data set of a casino-type viewable game, said
2 method comprising the steps of:
- 3 (a) providing a data set for a casino game;
- 4 (b) computing a first abbreviated bit string unique to the data set;
- 5 (c) encrypting the abbreviated bit string to provide a signature;
- 6 (d) storing the data set and the signature;
- 7 (e) computing a second abbreviated bit string from the stored data set;
- 8 (f) decrypting the stored signature to recover the first abbreviated bit
9 string; and
- 10 (g) comparing the first and second abbreviated bit strings to determine
11 whether the first and second abbreviated bit strings match.
- 1 2. The method of claim 1 wherein said step (b) of computing is performed with
2 a hash function to produce a hash value of the data set, and wherein said first
3 abbreviated bit string comprises the hash value of the data set.
- 1 3. The method of claim 2 wherein the hash value comprises the message digest
2 of the data set.
- 1 4. The method of claim 1 wherein said step (c) of encrypting is performed using
2 a private encryption key.
- 1 5. The method of claim 1 wherein said step (f) of decrypting is performed using
2 a public decryption key.
- 1 6. The method of claim 1 wherein said step (c) of encrypting is performed using
2 a private encryption key, and said step (f) of decrypting is performed using a public
3 decryption key.

- 1 7. The method of claim 1 wherein said step (e) of computing is performed with
2 a hash function to produce a hash value of the stored data set, and wherein said
3 second abbreviated bit string comprises the hash value of the stored data set.
- 1 8. The method of claim 7 wherein the hash value comprises the message digest
2 of the stored data set.
- 1 9. The method of claim 1 wherein said step (d) of storing includes the step of
2 storing the data set and the signature in a mass storage device.
- 1 10. The method of claim 9 wherein the mass storage device comprises a disk
2 drive unit.
- 1 11. The method of claim 9 wherein the mass storage device comprises a CD-
2 ROM unit.
- 1 12. The method of claim 9 wherein the mass storage is a network storage system.
- 1 13. The method of claim 1 wherein said steps (a)-(d) are performed at a first site, and wherein steps
2 (e)-(g) are performed at a second site.
- 1 14. The method of claim 13 wherein the first site comprises a manufacturing
2 facility, and wherein said second site is a gaming facility.
- 1 15. A method of preparing a casino game data set capable of authentication, said
2 method comprising the steps of:
3 (a) providing a data set for a casino game;
4 (b) computing a first abbreviated bit string unique to the casino game data
5 set;
6 (c) encrypting the abbreviated bit string to provide a signature; and
7 (d) storing the casino game data set and the signature.

(c) comparing the first and second abbreviated bit strings to determine whether the first and second abbreviated bit strings match.

1 29. The system of claim 28 wherein said mass storage device comprises a disk
2 drive unit.

[illegible]

1 37. The device of claim 36 wherein the message digest computing program
2 comprises a hash function.

[illegible]

1 38. The device of claim 36 wherein the stored decryption key comprises a public
2 key.

1 39. The device of claim 36 further including an initial loader program stored in
2 said unalterable read only memory device for ensuring use of the message digest
3 computing program, the decryption program and the decryption key.

1 40. A method of preparing casino game software information capable of
2 authentication, said method comprising the steps of:

- 3 (a) providing software information relating to a casino game;
4 (b) computing a first abbreviated bit string unique to the casino game
5 software information;
6 (c) encrypting the abbreviated bit string to provide a signature; and
7 (d) storing the casino game software information and the signature.

1 41. The method of claim 40 wherein said step (b) of computing is performed with
2 a hash function to produce a hash value of the stored casino game software
3 information, and wherein said first abbreviated bit string comprises the hash value
4 of the stored casino game software information.

1 42. The method of claim 41 wherein the hash value comprises the message digest
2 of the casino game software information.

1 43. The method of claim 40 wherein said step (c) of encrypting is performed
2 using a private encryption key.

1 44. The method of claim 40 wherein said step (d) of storing includes the step of
2 storing the casino game software information and the signature in a memory device.

1 45. A method of authenticating casino game software information having a
2 signature encrypted from a first abbreviated bit string computed from the casino
3 game software information, said method comprising the steps of:

7 (c) comparing the first and second abbreviated bit strings to determine
8 whether the first and second abbreviated bit strings match.

1 47. The method of claim 46 wherein the hash value comprises the message digest
2 of the casino game software information.

1 48. The method of claim 45 wherein said step (b) of decrypting is performed
2 using a public decryption key.

1 49. An electronic gaming system for providing authentication of software
2 information relating to a casino type game, said system comprising:

3 first means for storing casino game software information and a signature of
4 said casino game software information, said signature comprising an encrypted
5 version of a unique first abbreviated bit string computed from the casino game
6 software information;

7 second means for storing an authentication program capable of computing a
8 second abbreviated bit string from the casino game software information stored in
9 said first storing means and capable of decrypting an encrypted signature stored in
10 said first storing means to recover the first abbreviated bit string;

11 processing means for enabling the authentication program to compute an
12 abbreviated bit string from the casino game software information stored in said first
13 storing means and for enabling the authentication program to decrypt the encrypted
14 signature stored in said first storing means to provide a decrypted abbreviated bit
15 string; and

16 means for comparing the computed second abbreviated bit string with the
17 decrypted abbreviated bit string to determine whether a match is present.

1 50. The system of claim 49 wherein said first storing means comprises a memory
2 device.

1 51. The system of claim 50 wherein said memory device comprises a read only
2 memory.

1 52. The system of claim 50 wherein said memory device comprises a RAM.

1 53. The system of claim 49 wherein said second storing means comprises a read
2 only memory device.

1 54. The system of claim 53 wherein said read only memory device comprises an
2 unalterable memory device.

1 55. The system of claim 53 wherein said read only memory device includes a
2 first portion for storing that portion of said authentication program capable of
3 computing the abbreviated bit string from the casino game software information, and
4 a second portion for storing that part of the authentication program capable of
5 decrypting the encrypted signature.

1 56. The system of claim 53 wherein said second ROM portion is used to store a
2 decryption key.

1 57. The system of claim 49 wherein said casino game software information
2 comprises program information.

1 58. The system of claim 49 wherein said casino game software information
2 comprises a fixed data set.

650720:6661360

1 59. For use in authenticating casino game software information and a signature
2 encrypted from an original message digest computed from the casino game software
3 information; an unalterable read only memory device having stored therein a message
4 digest computing program corresponding to the message digest program used to
5 compute the original message digest of the casino game software information, and
6 a decryption program and decryption key corresponding to the encryption program
7 and encryption key used to prepare the encrypted signature of the original message
8 digest.

1 60. The device of claim 59 wherein the message digest computing program
2 comprises a hash function.

1 61. The device of claim 59 wherein the stored decryption key comprises a public
2 key.

1 62. The device of claim 59 further including an initial loader program stored in
2 said unalterable read only memory device for ensuring use of the message digest
3 computing program, the decryption program and the decryption key.

Add A1